Secure biometrics stops fraud across channels.

Leave fraudsters and identity thieves speechless with Nuance Security Suite.

Criminals love contact center agents because they are trained to be helpful. This makes contact centers an attractive target for fraudsters who can leverage the abundant information available on social networks. Fraud attacks, including account takeovers, Automated Clearinghouse (ACH) electronic payments fraud, and identity theft are a large and growing issue for businesses and consumers. In fact, account takeover losses contribute to 28% of global identity theft losses.

How do you stop increasingly sophisticated fraudsters from attacking your contact center? Fraudsters may already have your customer's favorite pet's name or date of birth. They may even be able to spoof caller ID, but one thing they can't do is speak with your customer's unique voice.

FraudMiner, a key component of the Nuance Security Suite, is a proven solution for fighting contact center fraud. By leveraging AI-powered, multi-modal biometric technology and targeted fraud detection techniques, Nuance helps organizations accurately identify the criminals behind account takeover attempts and stops fraudster activities across the company.

Key benefits

Mitigate direct financial losses by stopping known fraudsters. Detect and prevent fraudsters who repeatedly call your contact center impersonating your customers.

Prevent new fraud – Recognize and analyze suspicious behavior in real-time, using Intelligent Detectors to identify new fraudsters.

Reduce operational risk – Improve customer and agent satisfaction by preventing fraud before customers are affected without making your contact center reps security experts.

Increase productivity of your fraud team – Robust and flexible tools mean smaller teams can address more fraud exposure and higher value fraud situations.

Assist law enforcement – Capture strong evidence to assist in prosecution and prevent future attacks.

How it works

Nuance FraudMiner uses voice and behavioral biometrics along with Intelligent Detectors to identify potential fraudulent behavior in a contact center. FraudMiner compares a known fraudster's print (voice, behavioral or conversation)

~70%

of contact center fraud is perpetrated by the same actors, so blacklisting their phone prints is a useful measure for stopping fraudsters in their tracks.[3]

Key facts

- Account takeover losses contribute to **28% of the total identify theft losses** globally in the financial sector[1]
- **One out of every 867 calls** into a financial institution's contact center is a fraud call ($42,546 is the average loss per account from phone fraud)
- **92% increase** in phone banking fraud in the UK from 2014-2015[2]
- Voice biometrics can help **reduce the cost of fraud in the contact center by 90%**, and via the mobile channel by 80%

1 Note: Statistics taken from a market study on fraud related to customer interaction in banking and financial enterprises by Infinity Research, 2015

2 FRAUD THE FACTS 2016 (Financial Fraud Action UK) https://www.financialfraudaction.org.uk/

3 Litan, Avivah. Gartner, Inc. "Preventing Fraud in the Call Center with Phone Printing and Voice Biometrics" (Forbes 2014, June 18). www.forbes.com/forbes/welcome/?toURL=https://www.forbes.com/sites/gartnergroup/2014/06/18/preventing-fraud-in-the-call-center-with-phone-printing-and-voice-biometrics/&refURL=&referrer=#133610953584

NUANCE

to the print detected on a call to alert contact center agents in real time when a known fraudster is on the line. Additionally, FraudMiner analyzes the call in real time to identify potential unknown fraud cases like different people calling on the same account.

Key capabilities

ROI in under six months – ROI is easily determined by establishing KPIs around fraud reduction based on historical data. Benefits are clear on the first day and most organizations see ROI in less than six months.

Known fraudster alert prevents repeating fraudster – Detects known fraudsters within seconds of the call; alerts the contact center agent so they can take appropriate actions in real time.

Prevent fraud from unknown fraudster – FraudMiner uses Intelligent Detectors to analyze incoming calls for over 100 different biometric factors that create alerts and present them to the contact center agent so that the fraud team can intervene in real time to prevent fraud.

Intelligent detectors includes **Channel ID** to determine the channel type used during the interaction, **Network ID** that analyzes the network quality to detect suspicious changes, a **Geo ID** feature that identifies the country and city the device is associated with.

Anti-spoofing includes **ANI ID** that analyzes the meta data in a phone call to identify inconsistencies and determine phone number spoofing, **Synthetic ID** that detects a wide array of synthetic voice technologies, including those generated by DNNs, **Liveness ID** that detects voice recordings through intra-session voice variation liveness testing, **Playback ID** that detects voice recordings through audio anomalies created by the recording and playback process.

Nuance DevicePrint – non biometric print created per device. Enables the platform to detect mismatches that indicate on potential fraudulent call.

ConversationPrint™ – ConversationPrint™ detects new fraudsters and improves accuracy by identifying fraudulent activity based on choice of words and patterns of speech or writing during an interaction with a human or a virtual assistant. Speech-to-text, a core competency of Nuance, is applied to short speech segments to analyze vocabulary, sentence structure, grammar, and more that are unique for each individual.

Brute force attack detection identifies when a fraudster is calling multiple times to try and find an agent who can be socially engineered. When this is detected, the fraud team is engaged to take a closer look so that the voice can be placed on a black list to ensure the fraudster will be stopped in the future.

Enhanced tools to enable fraud investigation and prosecution – FraudMiner web applications can be used to manage fraudsters and watchlist entities, analyze suspicious audio and investigate fraud alerts according to their severity.

Backward search to uncover fraud – Uncover the identity and patterns of fraudsters using large-scale, historical search capabilities.

Keyword Spotting (KWS) to flag potential fraud – The fraud team can enable KWS to find specific sequences of words in the call recording, e.g. “I want to move x $ from my saving account to this credit card”, “I want to change my address”. This can greatly reduce the amount of time the fraud team has to spend identifying potential fraudsters.

Market leading technology

Nuance delivers a comprehensive, state of the art technology for fraud and authentication that works together seamlessly on a common platform to mitigate direct financial losses.

For more information about FraudMiner go to www.nuance.com/security-suite.

About Nuance Communications, Inc.

Nuance Enterprise is reinventing the relationship between enterprises and consumers through customer engagement solutions powered by artificial intelligence. We aim to be the market leading provider of intelligent self- and assisted-service solutions delivered to large enterprises around the world. These solutions are differentiated by speech, voice biometrics, virtual assistant, web chat and cognitive technologies; enabling cross-channel customer service for IVR, mobile and web, Inbound and Outbound; and magnified by the design and development skill of a global professional services team. We serve Fortune 2500 companies across the globe with a mix of direct and channel partner selling models.

NUAN–CS–3016–02–DS, Jun 20 2018